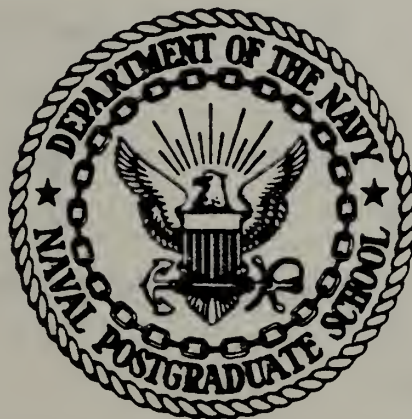


DUDLEY KNOX LIBRARY
NAVAL FOR
NEW YORK 93143

NAVAL POSTGRADUATE SCHOOL

Monterey, California



THESIS

NEEDLS AND HAYSTACKS:
THE SEARCH FOR ULTRA IN THE 1930's

by

Linda Yolande Gouazé

March 1983

Thesis Advisor:

S. Jurika

Approved for public release; distribution unlimited

121,179

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Needles and Haystacks: The Search for Ultra in the 1930's		5. TYPE OF REPORT & PERIOD COVERED Master's Thesis; March 1983
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Linda Yolande Gouaze		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93943		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, California 93943		12. REPORT DATE March 1983
		13. NUMBER OF PAGES 84
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) Enigma British Intelligence code-breaking World War II Polish Intelligence intelligence French Intelligence cryptology		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) This thesis traces the efforts in the 1930's of the Polish, French, and British Intelligence Services to break the German Enigma ciphering machine, efforts which led to the Bletchley Park Ultra operations of World War II. The cooperation, and lack thereof, among the Intelligence Services is discussed, with the conclusion that more cooperation sooner would have better served the individual national interests of each.		

DD FORM 1473
1 JAN 73EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-LF-014-6601

UNCLASSIFIED

1
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

Approved for public release; distribution unlimited

NEEDLES AND HAYSTACKS:
THE SEARCH FOR ULTRA IN THE 1930's

by

Linda Yolande Gouaze
GS-13, Department of Defense
B.A., Seton Hill College, 1965
M.S.S.I., Defense Intelligence School, 1981

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN NATIONAL SECURITY AFFAIRS

from the
NAVAL POSTGRADUATE SCHOOL
March 1983

ABSTRACT

This thesis traces the efforts in the 1930's of the Polish, French, and British Intelligence Services to break the German Enigma ciphering machine, efforts which led to the Bletchley Park Ultra operations of World War II.

The cooperation, and lack thereof, among the Intelligence Services is discussed, with the conclusion that more cooperation sooner would have better served the individual national interests of each.

TABLE OF CONTENTS

I.	INTRODUCTION - THE ENIGMA MACHINE -----	6
	CHAPTER I END NOTES -----	13
II.	NEEDLES AND HAYSTACKS -----	14
	CHAPTER II END NOTES -----	19
III.	THE NEEDLES ARE THREADED (1925-1938) -----	20
	A. GENERAL -----	20
	B. THE POLISH NEEDLE -----	21
	C. THE FRENCH NEEDLE -----	28
	D. THE BRITISH NEEDLE -----	36
	E. THE PICTURE THROUGH 1938 -----	39
	CHAPTER III END NOTES -----	41
IV.	THE THREADS CROSS (JANUARY - AUGUST 1939) -----	47
	A. THE PARIS MEETING (9-11 JANUARY 1939) -----	47
	B. BUSINESS AS USUAL (FEBRUARY - JUNE 1939) -----	49
	C. THE WARSAW MEETING (24-25 JULY 1939) -----	51
	D. ANOTHER STORY -----	52
	CHAPTER IV END NOTES -----	56
V.	APRES CA, LE DELUGE (SEPTEMBER 1939 - MAY 1945) -----	57
	A. THE THREADS JOIN (SEPTEMBER 1939 - JUNE 1940) ---	57
	1. The Pattern Forms (September 1939 - December 1939) -----	57
	a. The Polish Needle -----	58
	b. The French Needle -----	60
	c. The British Needle -----	61

2. The Pattern Blurs (January 1940 - June 1940) -	63
B. TANGLED THREADS (JULY 1940 - DECEMBER 1942) -----	67
C. THE ENDS (JANUARY 1943 - MAY 1945) -----	70
CHAPTER V END NOTES -----	72
VI. CONCLUSIONS -----	75
CHAPTER VI END NOTES -----	78
BIBLIOGRAPHY -----	79
INITIAL DISTRIBUTION LIST -----	84

I. INTRODUCTION - THE ENIGMA MACHINE

This study traces the pre-World War II efforts of Polish, French, and British intelligence organizations to acquire and read Nazi communications enciphered on the electro-mechanical Enigma device. Since the study examines those efforts in a historical and human context, no technical explanation of the cryptanalytic processes is included within the text. Yet, in order to follow the unfolding story, some description is needed of the scope of the Enigma problem these organizations faced. The following paragraphs are essentially a distillation of the already admirably non-technical explanations of the principles and cryptanalytic difficulties of Enigma provided by Ronald Lewin¹ and Peter Calvocoressi.²

The Enigma machine resembled a primitive electric typewriter and, in grossly oversimplified terms, operated in somewhat the same way. Depressing a key on the keyboard generated an electrical pulse that, rather than causing the selected letter to be imprinted on paper, caused a different letter to light up on a second "keyboard." That second letter was then used in the cipher text to replace the original letter. Had the process been that simple, however, the Germans would not have believed their communications to be so secure, and many fewer books would have been written about the Allied cryptanalytic successes against Enigma.

The difficulty that makes the Enigma story astounding was caused by the interposition of various complicating devices between the first and second keyboards, and by the fact that these devices caused a different cipher letter to be selected for a given key each time it was pressed. That is, the first time A was pressed it might become Q, but the next time it would be L or Z or anything but Q.

For example, the maze of wiring through which the electrical pulse had to travel was partly distributed on three rotating wheels or rotors.³ Each wheel contained entry and exit points on its rim for 26 letters. Each was wired differently and the wheels could be placed in any order in the machine, giving a possibility of six different wheel combinations for three wheels.

When a letter on the keyboard was struck, the electrical impulse travelled a crazy route through the three rotating wheels, struck a reflector and travelled back by a different route through the same three still-rotating wheels.

Also, by 1930 plugs (somewhat like those on an old-fashioned telephone switchboard) were added to the machine to link pairs of letters and thus further vary the path a given electrical impulse would travel between the two keyboards.

German units which were to encipher and decipher messages using the Enigma machine were provided with lists of settings for the beginning positions of the rotors and plugs for use

during specified periods. If both sender and receiver set the machine up properly according to these lists, the receiver would type the cipher text into the machine, and the original plaintext letters would light up.

Besides these purely electro-mechanical complications, there was also a key embedded at the beginning of each message which indicated the initial positions of the three wheels, e.g., first wheel set at A, second at L, third at C. These three-letter groups were provided by the same handbook that gave the wheel orders and plug connections for a specified 24-hour period. The three-letter group was enciphered twice at the beginning of the message (hence, a preambular key), e.g., ABCABC might become QULBDR.

The problem faced by cryptanalysts in the late 1920's and early 1930's, then, was essentially: first, to deduce the basic wirings of the wheels and plugs; and second, to devise ways of determining wheel orders and plug settings and the preambular key for a particular day.

Nothing is known about British or French approaches to this problem, except that they were apparently not successful, but it is known that it was attacked by Polish cryptanalysts as a problem in theoretical mathematics. They constructed an equation describing Enigma's permutations - the number of different states in which the machine might be at any given moment - and then solved it by establishing and then exploiting, certain critical mechanical facts about the

wheel operations. Since the total number of theoretical permutations was above the billions - Calvocoressi notes the figure contained 88 digits⁴ - the solution and consequent reconstruction of the Enigma machine in Poland represents an incredible feat.

Having once done this, however, the cryptanalysts still had to determine the daily settings and key. This was theoretically possible if all of the possible permutations were tested, but obviously impractical if it was intended to decipher messages in the same century in which they were enciphered - especially since all early deciphering was done by hand.

The obvious point of attack was the preambular key. Given a 26-letter alphabet, there were "only" 17,576 possible sets of three-letter groups. Also, review of intercepted German messages revealed that identical sets of three-letter groups were turning up more often than chance would dictate, which implied that some German operators were violating the rules of randomness by using standard groups, like AAA, ABC, or German words like IST or VON. Since the key was doubly enciphered, if for example, ABCABC or ISTIST were used, the cryptanalysts knew that the first and fourth, second and fifth, and third and sixth letters were identical. Using these hints, the cryptanalysts made sufficiently educated guesses to reduce to manageable proportions the time required to solve a daily setting and key.

Calvocoressi notes⁵ that faulty operating procedures - such as the double encipherment of the preambular key - and failures to observe the rules - such as using common three-letter groups or words as keys - were ultimately the only two practical ways into the Enigma system.

Prior to September 1938, these two methods were successfully used by the Poles for more than six years to read German Enigma traffic. In September and December 1938, however, the Germans introduced two changes which effectively shut the Poles out of Enigma, not because of a theoretical or technical inability to solve the changes, but because of a lack of time and money to develop appropriate aids to solve them fast enough for practical purposes.

The first change was procedural: instead of a single designated preambular key for all messages in a 24-hour period, German operators were directed to select their own random three-letter groups, and to use a different one for each message. Therefore, solving a key would permit only one message to be read rather than all the messages for that day.

The Poles were well on their way to solving this new problem, by devising and constructing additional aids to speed up the testing process (such as the perforated sheets and the Polish "bombs"), when these processes were thrown into a cocked hat by a technical change in December 1938: two additional rotors were made available to operators, so that any three of five differently wired wheels could be

emplaced on the Enigma machine at one time. The Poles deduced the wirings of these two wheels successfully, but were unable to exploit them. Now, instead of six possible wheel orders to test for daily settings, there were sixty. Therefore, the "bombe," which consisted of parts of six Enigmas wired together in such a way as to test the six possible wheel orders quickly, would require 60 Enigmas. And the other primary aid, the perforated sheets, would require 60 series of laboriously hand drawn and cut sheets rather than the six that previously sufficed. The Poles lacked the economic resources to create the aids they knew were required so that, although they had been reading German Enigma traffic for years, they were now shut out of Enigma⁶ until January 1940, when the first Allied break into Enigma was made by Poles located at a French cryptologic center on British-manufactured copies of the Polish perforated-sheet design.

This, then, was the scope of the Enigma problem, and the nature of the attacks against it. Although the British virtually redesigned the "bombe" and invented other more sophisticated mechanical and electronic aids, they all were designed to speed up the testing process for the approaches used originally by the Poles: they exploited faulty operating procedures such as double encipherment of the preambular key (until this was cancelled by the Germans in May 1940), and they exploited the German operators' violation

of procedural rules, either by use of "cribs" - guessing of common three-letter groups in keys or of standard words or phrases elsewhere in a message - or because a message had been enciphered both in a lower-grade cipher and in an Enigma cipher. A break into the simpler low-grade cipher then gave one a break into Enigma for that day.

As to the prize that resulted from all of these efforts, the quality and volume of intelligence on German order-of-battle, movements, and intentions have been amply described in the many excellent works not available on wartime counter-Enigma operations.

CHAPTER I
END NOTES

1. Ronald Lewin, Ultra Goes to War: The First Account of World War II's Greatest Secret Based on Official Documents (New York: Pocket, 1980), pp. 8-21.
2. Peter Calvocoressi, Top Secret Ultra (New York: Ballantine, 1981), pp. 23-39, 53-59.
3. There was also a fourth stationary wheel which operated as a reflector. Until an Enigma with four rotating wheels was introduced in the German Navy in 1943, all Enigmas utilized only three wheels at a time, though sometimes those three could be selected from among a larger number available.
4. Calvocoressi, p. 29.
5. Ibid., p. 54.
6. Actually, the Poles continued to read a small part of the Enigma traffic - that of the SD (Sicherheitsdienst) - until July 1939, when the SD's procedures were brought into line with those of the other Enigma users.

II. NEEDLES AND HAYSTACKS

Since 1973, Enigma/Ultra literature - comprising both memoirs and scholarly analyses - has grown enormously. While many of these works have helped to clarify the use and impact of Enigma decrypts during the war, every additional book or article adds as much confusion as clarity to the pre-war period of the Enigma/Ultra story, when the Intelligence Services of at least three countries were pursuing this outstanding source. At this point, any publication which recounts "Ultra's pre-history"¹ in the 1930's and early 1940's is essentially reduced to selecting among the several, and often contradictory, versions available from participants.

This is due largely to three major factors: a lack of available official documentation from the pre-war and early war years, the time-honored intelligence principle of need-to-know, and the enormous complexity of a situation of which each participant saw only a small part.

Although a wealth of official and unofficial material has now been released or written on Enigma, no documentation prior to 1940 has reached the public domain, which could confirm or deny the specific events cited by the various authors. Therefore, one author states firmly that British Enigma operations at Bletchley Park (known hereinafter and to habitues as B.P.) grew from an Enigma machine stolen by

the Polish Intelligence Service on behalf of the British Intelligence Service,² while others convincingly describe independent Polish reconstruction and exploitation of Enigma, with some documentary assistance from the French and a subsequent gift of the Polish accomplishments to Britain and France.³ As recently as 1982, Gordon Welchman's memoirs allow the casual reader to believe that all stories may be correct.⁴ While I don't completely agree with Gordon Welchman, (see pp. 52-56 below) the absence of any solid documentation from this period, such as reports filed at the time by participants, makes absolute refutation of any story impossible. That is, while it may be possible in some cases to establish plausibly that an event probably did happen (as Gustave Bertrand "proves" with dated postcards that he was in Latvia and Lithuania on certain relevant dates⁵), it is generally not possible to prove that a specific event did not happen somewhere in the netherworld of intelligence.

The material released from official sources thus far seems to follow a pattern so traditional in the intelligence profession that it has the force of "law". National interest/prestige, political considerations from national leaders, etc., may require the release of information and/or documentation on intelligence facts, processes, use, or impact, but never never on the sources from which it was derived or the methods by which it was extracted. Therefore, Bertrand's 1973 book concerned Polish sources and methods but, except

for a German spy who was shot in 1943, does not reveal much about French intelligence operations.

Likewise, Winterbotham's book essentially begins at the point where the Enigma ciphers were already broken, and continues with information on the dissemination, use, and impact of the intelligence which resulted. That later British writers have discussed some details of the deciphering procedures can be attributed to the third group of participants, the Poles.

This group was in a unique position by the time information became public; they were writing about sources and methods of intelligence acquisition in and for a nation-state which effectively no longer existed. Consequently, feeling no continuity between those events and the present government, they presumably did not feel bound by some of the unwritten laws as did the British and the French.

Unfortunately (if one is a historian), the release of official data to the public has followed essentially the same lines: the French have released nothing, and the British little besides the intercepts and decrypted messages that resulted from the complex international intelligence collection operation that preceded it. The Poles involved have provided such information as they recall or for which they have records, but can hardly be expected to have carted large amounts of collateral documentary evidence out of Warsaw with them in September 1939.

Adding to the "fog of battle" in writing on the history of intelligence is another time-honored principle of the profession: need-to-know. If the "sources-and-methods" rule can be described as a way of ensuring the protection of the most important aspects of an intelligence operation (in effect, protecting the goose more stringently than its golden eggs), then the "need-to-know" rule is a broad-brush way of limiting the damage which any one individual can cause to the goose, its eggs, the house it lives in, and its owners. That is, theoretically at least, no-one has any more pieces of information about any intelligence operation than he or she needs to do his or her part successfully.

In the Enigma/Ultra operation, this means that no one person writing from his own experiences as a participant could possibly provide a complete picture. Each is hamstrung in describing his own service's participation by the need-to-know principle; and completely defeated in even hazarding a guess about another country's participation by the sources-and-methods principle, which operates nearly as well against another country's intelligence service, even if friendly, as it does against releasing information on sources and methods to the public.

The limitations of view of the participants involved, caused largely by the rules of the intelligence game, then, have thus far precluded a balanced critical recounting from any of the "insiders" in the exceedingly complex developments

of an already very shadowy arena. From British, French, or Polish tales of these events, the impression derived is that the Enigma successes were due essentially to a single country's efforts, with occasional and usually trivial assistance from the other two countries.

Actually, probably the most important premise in understanding developments in the collection and initial exploitation phases of the Enigma story is that the framework of the story is one of three totally separate and distinct efforts under way throughout the 1930's, one Polish, one French, and one British. Although these efforts had the same goal - use of decrypted Enigma messages to gain intelligence on Nazi Germany - none was begun or continued purely as a partnership. Each of the countries involved did what was necessary to advance its own intelligence collection and exploitation program against Enigma, cooperating with the others (i.e., sharing anything acquired or developed within the Service) only whenever and however it appeared to be useful in advancing its own program and contributing to its own national security.

What follows, then, is an attempt to find three individual needles in three separate and complex haystacks, and to follow the threads attached to each of the needles to discover where they cross, join, and end.

CHAPTER II
END NOTES

1. Lewin, p. 11.
2. F.W. Winterbotham, The Ultra Secret (New York: Harper and Row, 1974), pp. 10-11.
3. Jozef Garlinski, Intercept: The Enigma War (London: J.M. Dent & Sons, Ltd., 1979), pp. 12-27, 33-47).
4. Gordon Welchman, The Hut Six Story: Breaking the Enigma Codes (New York: McGraw-Hill, 1982), pp. 13-16.
5. Gustave Bertrand, Enigma, ou la plus grande enigme de la guerre 1939-1945 (Paris: Librairie Plon, 1973), p. 41.

III. THE NEEDLES ARE THREADED (1926-1938)

A. GENERAL

As with any intelligence collection operation, the efforts against Enigma began with the identification of the target - in this case, the introduction in 1926 of the Enigma ciphering machine into the German Armed Forces.

While the potential of electrically-operated ciphering machines for providing a secure means of communications was being investigated by other major countries in the 1920's, Germany was apparently the first to adopt one as standard issue throughout its governmental operations. First of its armed forces to employ Enigma was the Navy, in 1926, followed by the Army in 1928, and the Air Force in 1934.¹ By the start of the war in 1939, most high-level German military communications, as well as those of the German diplomatic corps and of intelligence agents abroad, were either encrypted by Enigma machines prior to transmission or carried by landlines.

This commonality may have made the Allied cryptanalysts job somewhat easier than if there had been a variety of machines in use, but it did not mean that a single break into Enigma gave access to all German communications. Each of the services utilized somewhat different versions of the Enigma, and there was a wide variety of codes in use, as well as difficulties presented by the changeable settings utilized to encode during different time periods.

The Germans, who had done considerable testing of the security aspect of Enigma prior to adopting it for broad high-level use, were probably theoretically justified in believing that the Enigma-based ciphers were invulnerable unless one had the machine, the keys, and the current setting for those keys.² Unfortunately for the long-range goals of the Third Reich, the Poles were able to gain continuing "possession" of all three items by reconstructing them through a small French hook into the German Cipher Office, brilliant Polish theoretical work, and sloppy German operational practices. Not one of these three factors could have permitted the astounding success eventually enjoyed throughout the 1930's by the Poles and throughout the war years by the British; all three were necessary to enable continuing success against the Enigma ciphers.

B. THE POLISH NEEDLE

The Enigma history from the Polish perspective is based almost entirely on memoirs written in the late 1960's and 1970's, although some material dates from as early as 1940.³ The absence of official documents from the 1930's is not due, in this case, to an unwillingness to release intelligence-related material to the public, but to the not surprising fact that most if not all records of the Enigma operation were destroyed in September 1939 to ensure that the Nazi conquerors did not learn of the Polish success.⁴ The major

documents providing the Polish perspective are reminiscences by Marian Rejewski, one of the three cryptologists who solved Enigma, his several responses to authors working in this area,⁵ and a lengthy memorandum written in May 1974, and supplemented in December 1974, by Colonel Stefan Mayer, Chief of Polish Intelligence during the 1930's and, in London, during the war years.⁶ Colonel Mayer notes that his memorandum is based on his memory to some extent, but also on some papers left to him by a more immediate participant in the Enigma story, Lt. Col. Gwido Langer, Chief of the Cryptologic Bureau of Polish Intelligence.⁷ Langer's papers include a report on specific cipher work done by his unit in France between September 1939 and June 1940,⁸ as well as some reminiscences written in 1946 in London.⁹ These materials form the basis for all accounts published thus far on the Polish side, except insofar as French and British writers have written their perceptions of Polish activities as they recalled them.

In reviewing the Polish side of the Enigma story, it is well to remember the general situation of that nation between World War I and World War II.

Poland had been established, divided, subjugated, and liberated at various times since its period of greatness in the 18th Century. It regained its independent national identity yet again in 1918, but was well aware that its independent status would be difficult to maintain from its

geographic position, sandwiched between its two traditional conquerors: Prussia, now incorporated into Germany, and Russia, now Bolshevik rather than Czarist, but still a threat to a poor and militarily weak Poland.¹⁰

The reality of the Russian threat to Poland was proven by the war of 1920-1921, when Poland's cryptologic success contributed significantly to the Polish victory.¹¹

Although both Russia and Germany were economically and militarily weak during the 1920's, either or both were sufficiently threatening to an even poorer and weaker Poland to cause the latter to keep close tabs on the political and military developments of its traditional enemies. Lacking the economic and military strength to defend itself through classic means, Poland emphasized relatively cheap methods in which individual skills had reaped critical benefits in its past: intelligence and diplomacy.¹²

Diplomatic efforts generally sought to keep Poland on reasonably good terms with its neighbors, and to establish and maintain alliances with nations which had the military strength to compensate for Poland's weakness. Maintenance of the traditional Polish-French ties falls in this latter category. A close diplomatic and military relationship with Great Britain, on the other hand, was not traditional; the alliance which existed during World War II dated only from 1939.

In the intelligence realm, Poland's exposed geographic position caused it to focus most assiduously on activities in Germany and Russia,¹³ and Poland may have been the first nation to note signs of what was the worst possible development from Poland's point of view: a growing rapprochement between its two traditional enemies.¹⁴ This closeness between Russia and Germany would have caused even more emphasis to be given by the Polish government to any means which might improve its knowledge of the capabilities and intentions of its two potential adversaries. Given Poland's location between Russia and Germany, and traditional Polish expertise in cryptology, intercepted and deciphered radio communications was a logical area of focus.¹⁵

In this context, it is not surprising that the appearance of the Enigma machine in the German Armed Forces in 1926 was soon recognized as potentially shutting off what had been a very lucrative source of intelligence on Germany.¹⁶ Polish intelligence focussed quickly on deciphering this new style of cipher, but to no avail.¹⁷

Whether from a greater consciousness of relative poverty (i.e., they couldn't throw money at the problem in hopes of simply overwhelming it) or from a greater sense of dangerous geographic exposure, or for some other reason, the Poles then took an approach that apparently didn't occur to the French or the British: they went outside their small corps of cryptologists to recruit fresh mathematical talent, possibly

on the assumption that an entirely new kind of cipher might best be broken by an entirely new approach to deciphering.

To this end, a cryptology course was organized in 1929 for the best of the higher mathematics students at Poznan University. The three top graduates of that course, Jerzy Roczyki, Henryk Zigalski, and Marian Rejewski, were then offered jobs in the cryptology section of the Intelligence Service.¹⁸

After some time spent on traditional hand ciphers, in October 1932, Rejewski was told to work on a "new" cipher separately from his two colleagues, who joined him two months later. He made some progress in determining the principles involved in the cipher, and has indicated that he was also helped somewhat in initial familiarity with the general operating principles of the machine by examining a commercial model.¹⁹

On 8 or 9 December 1932,²⁰ one Captain Gustave Bertrand, Chief of the French Army Intelligence Service's Cryptology Section, provided several documents, acquired from the German Cipher Office by a spy, describing some of the technical characteristics of the military Enigma. By the end of that month, Enigma was broken.²¹ The security of the vaunted impregnable machine-based cipher had been breached by three inexperienced young cryptologists and a couple of stolen instruction documents.

From then until September 1938, the Polish cryptologists proved equal to every procedural change the Germans introduced. By January 1938, according to Col. Mayer and Marian Rejewski, their reading of Enigma traffic was so routine and current that Col. Mayer measured a 75% success rate in a 2-week test in which he randomly selected incoming intercepts to be deciphered.²²

Interestingly, but typical of dealings between intelligence services of different countries, the Poles apparently never told the French during this time of their success in breaking Enigma. Whatever the specific agreement may have been when Bertrand turned over the Enigma documents, it is probably fair to assume that the French expected to share in any progress or success against Enigma.²³ Since the documents turned over in December 1932 were all the French had to offer, however, there was nothing further to be gained from the Polish perspective by giving the French access to the results of the Polish attack on Enigma. So, the "family jewels" were kept within Polish channels.

There was some continuing cooperation with the French and with the Czechs, though apparently not with the British. Raw (i.e., undeciphered) intercepts were exchanged among the French, Czech, and Polish cryptology units, possibly as early as Bertrand's visit to Poland and Czechoslovakia in December 1932,²⁴ and this exchange system was developed into a communications network in 1938.²⁵ The network was called

BLR, after the code names of the three cryptology chiefs: Bertrand was Bolek, Lt. Col. Gwido Langer of Poland was Luc, and Frantisek Moravec of Czechoslovakia was Raoul. Communication was by radio;²⁶ although no information is available on the location or nature of the Czech and French reception points, the Polish leg of the triad was located in the Pyry Forest near Warsaw, adjacent to the concrete blockhouse-type structure that housed the Polish Enigma efforts.²⁷

By December 1938, the efforts against Enigma in the Pyry Forest had been somewhat systematized. Several aids had been invented and manufactured to assist and speed-up the deciphering efforts. These included a mechanical contrivance, the "bombe", which was an electro-mechanical lash-up of parts of six Enigma machines that could rapidly test possible combinations of letters in an Enigma key.²⁸ In addition, there were "improved" hand methods, such as the so-called "perforated sheets", which were 51x51 charts of letters (26 sheets to a set), with holes distributed in such a way that proper stacking of the sheets would result in the correct letter being revealed by a direct line of holes in each sheet.²⁹

As happens all too frequently in intelligence, however, just as the Poles had collection, exploitation, and production of this intelligence working just right, the rest of the world shifted gears, throwing the Polish efforts into considerable disarray, and rearranging their alliance structure somewhat.

Disarray in the Enigma deciphering system was caused by two kinds of changes introduced by the Germans during 1938: in September substantial procedural changes were made, which shut the Poles out for about two months, and in December a much more damaging change occurred when two rotors were added to the Army and Air Force Enigma. This change effectively shut down all intelligence from Enigma deciphers until January 1940, because the Polish mechanical and paper aids were rendered useless. They required redesign and remanufacture, with the number of partial Enigma machines required for a "bombe," for example, going from 6 to 60. Besides being a time-consuming process, this remanufacture was prohibitively expensive for a country as poor as Poland, and was not completed prior to Poland's defeat in September 1939.³⁰

The situation faced by Poland's cryptology unit also changed in other ways. The Anschluss in March 1938 and the Munich Pact in September 1938 generated enough concern that a previously reluctant element was added to the Enigma equation: Great Britain. There is no indication that any cryptologic cooperation with Great Britain ensued in 1938, but the stage was set for the considerable cooperation that took place later.

C. THE FRENCH NEEDLE

Like the Polish role, the French part in the Enigma story is visible through memoirs, specifically those of Gustave

Bertrand, Chief of the French Army Intelligence Service's Cryptology Service from 1930 to 1944; Paul Paillole,³¹ who was a member and then Chief of its Counterintelligence Section from the mid-1930's to 1944; and Henri Navarre,³² who was a member and then Chief of its German Intelligence Section from the early 1930's to 1944.

Unlike the Poles, however, the lack of official documentation from France is apparently due to a decision not to release any material from the intelligence services for 60 years³³ vice the 30-year date set for other types of World War II documentation. It is doubtful that complete documentation still exists on French participation in the Enigma affair, since many intelligence files were probably destroyed as the Germans approached Paris. Bertrand notes in his memoirs, however, that some of his section's files were evacuated to the Vichy Zone in June of 1940,³⁴ hidden locally prior to German-Italian occupation of the Vichy Zone in November 1942,³⁵ and recovered in 1945.³⁶ There may be a considerable amount of information added to the Enigma history when these files become available to researchers in 2000.

This apparently strong tradition of non-release of intelligence data may form part of the basis for the general flavor of disapproval and rejection of Bertrand's story that one gets in France. Additionally, it would appear that Bertrand's personality and some of the opinions expressed in his book did not endear him to his fellow officers.³⁷ For

example, in Bertrand's memoirs he states that he was the architect of the entire Enigma operation.³⁸ He occasionally makes slighting remarks about his superiors, constantly refers to his own individual actions or requests to his superiors to act independently (which were usually granted) and implies that he, personally, was the moving force behind all of the French activities.

Since his superiors are all long since dead, it is very difficult to determine with any degree of certainty just how much of the French participation was due to Bertrand, or whether he simply participated as the Chief of the Cryptology Section but at the behest or direction of his superiors.

It is interesting to note, however, that no author on this subject has provided any other names or any indications that the actions that Bertrand attributes to himself were in fact taken or directed by any other quarter.³⁹

As Bertrand is no better liked in England than he is in France, one might expect that some of the British who were acquainted with French participation would have specifically attempted to attribute some of his actions to other French officers. Even those who excoriate him the most, such as Ronald Lewin, whose few comments on Bertrand resemble a personal attack more than an objective scholarly analysis,⁴⁰ do not seem able to mention another leading French officer.

Whatever the justice of Bertrand's claims to have acted independently, or of the criticisms of the British and French

authors who suggest that he was not quite the kingpin he implies, the negative reaction to his book leaves Bertrand and the entire French role as a somewhat forgotten element in the Enigma story.

It is true that the French Intelligence Service did not make any of the technical breakthroughs; it also did not apparently make any great operational contributions, either to breaking the Enigma ciphers or to the periods of combat prior to the fall of France. However, Bertrand and the French Intelligence Service appear to have acted as the catalyst which enabled the entire operation to be successfully concluded. This catalytic role occurred first in December 1932 when Bertrand gave the Asche documents to the Poles and to the British,⁴¹ without apparently requiring that anything be given the French in return. The Poles, as described earlier, used these documents to very good effect. Oddly enough, the French apparently were unable to make any practical use of them, and there is no evidence that the British did, either.

France was a "winner" in World War I, but exhausted by its victory. After that experience with Germany, the French were conscious of a need to watch their eastern neighbor and devoted a substantial portion of their intelligence effort to collecting intelligence on Germany.

Like the Poles, the French came out of World War I with a good reputation for "radio intelligence" and cryptology.

Also like the Poles, this experience with hand ciphers did little to prepare them to deal with the Enigma-based ciphers when they appeared in German communications after 1926.

There is no information available on early French attacks on the Enigma ciphers, but Bertrand's book implies that no progress had been made by the time he took over as Chief of the Cryptology Section in 1930.⁴²

Bertrand notes that he immediately set about gathering information on Enigma,⁴³ which is probably true, since the gradual shutdown of a previously lucrative intelligence source would logically have been the greatest problem facing any chief of cryptology. Interestingly, he seems to have focussed on procuring collateral information to provide a hook into the system rather than on theoretical efforts directly aimed at breaking it, as the Poles did. This impression may simply be the result of 20-20 hindsight, but there is no indication that any direct attack was mounted by French cryptologists.

The first - and only - break in the French search for information came in late 1932, when a young German offered to provide French Intelligence with documents from the German Army's Cipher Office (Chiffrierstelle, often abbreviated to Chistelle), where he worked. Bertrand reports that the initial reaction by French Intelligence was that "the bride is too beautiful"⁴⁴ - too good to be true - describing someone who spontaneously offers such valuable material that

one worries that he may be an agent of his own country seeking to plant false information in an opposing service. His French code name was Asche⁴⁵ and, although recent analysis indicates that he was one Hans-Thilo Schmidt,⁴⁶ Asche will be used in this paper since it is the name used in most works on Enigma.

Asche was the "property" of Navarre's German Intelligence Section, which handled all German agent intelligence, but, since his area of potential use was cryptology, Bertrand was called in, perhaps initially to assess his ability to provide useful information on German ciphers, and then to receive Asche's material and give him guidance on what further information should be acquired and brought to the next meeting. Bertrand, accompanied by various officers from Navarre's section, by another agent, Lemoine (who may have acted as interpreter), and by a photographer (who copied Asche's documents on the spot), had a total of 19 meetings with Asche.⁴⁷ During these meetings, Bertrand received some 303 cipher-related documents from Asche. Only a few of these were concerned specifically with the Enigma system, but two or three of those few turned out to be highly valuable.⁴⁸

Bertrand, apparently feeling that it would take a concerted effort on the part of several countries' intelligence services to breach this seemingly impregnable system, set out to visit the countries that might be expected to see Germany as a significant threat: Czechoslovakia, Poland,

Latvia, Lithuania, Estonia, and Great Britain.⁴⁹ In the great tradition of intelligence described earlier, his purpose was not simply to pass out the Asche material to whomever had a use for it, but to assess the ability and willingness of each of the countries visited to protect the Asche documents from compromise and to use them in contributing to a solution of the Enigma system. Thus, the underlying purpose was, as always, primarily to ensure the security of his own country, and to assist others in their own security only as a means of achieving the primary goal.

As a result of Bertrand's assessments of these countries, the Asche documents were given only to Poland and Great Britain, which appeared to have the greatest potential capability to contribute to a solution. An agreement to exchange intercepts was made with Poland and with Czechoslovakia, which apparently had a lesser cryptologic capability, while Lithuania and Estonia, which indicated no familiarity or capability for signals intelligence work, were simply dropped from his list of potential partners.⁵⁰

Poland and Czechoslovakia collaborated with France in exchanging intercepts throughout the 1930's, but Great Britain showed no interest at that time.⁵¹ One may presume that French cryptologists also made some attempts against Enigma during the 1930's, but apparently without success.

After the Anschluss in March 1938 and the Munich Pact in September 1938, concern about German intentions was naturally

intensified throughout Europe, and the British showed an increased interest in collaboration. By the end of 1938, Bertrand and the British were apparently very worried at the perceived lack of progress by the Poles, whom they seem to have recognized as the strongest contenders for a solution.

Bertrand, believing that neither the Poles nor the British had any more success against Enigma than the French, proposed to Langer that a deception operation be run to convince the Germans that Enigma had, in fact, been broken, and thereby force them to discard Enigma and spend considerable time, effort, and money adopting some new system. He thought that this would effectively delay any immediate plans for war that the Germans might have, since one cannot go to war believing that enemies are privy to one's high-level military and diplomatic communications.⁵²

Interestingly, some authors on Enigma/Ultra have mentioned Bertrand's proposal with scorn. Lewin, for example, describes it initially as a shameful proposal (though understandable from a wimp like Bertrand), then reverses himself later in the same paragraph and notes it's not such a bad way to salvage some benefit out of a failed cryptologic effort.⁵³

Langer, of course, advised against this procedure, since he knew full well that Enigma had been broken for years, so Bertrand instead proposed a meeting in Paris in January 1939 of cryptologists from all three countries, to discuss the Enigma problem and attempt to pool their efforts to speed up a solution.⁵⁴

D. THE BRITISH NEEDLE

World War I was also an exhausting experience for the British. Unlike the Poles and the French, however, Britain's relatively greater distance from Germany and sense of protection afforded by the English Channel may have permitted a bit longer self-indulgence in ignoring the growing power of Germany. There are some indications that this ostrich-like attitude was not held by British Intelligence. Winterbotham, for example, notes that for part of the 1930's he was unable to convince government policy-makers that Germany might constitute a threat.⁵⁵

British Intelligence had also come out of World War I in a strong cryptologic position, but had, of course, no more experience than any other country with breaking machine-based ciphers. How seriously and how early British Intelligence focussed on the Enigma problem is difficult to determine, due to the lack of information in the public domain.

Although Great Britain is the only one of the three countries involved to release official documents concerning Enigma/Ultra to the public, this release appears limited to wartime documentation, i.e., after 1 September 1939. Therefore, the British side of this story during the 1930's is also largely limited to recollections, but with an added twist that makes the early British efforts against Enigma much more obscure than those of the French and Polish services: all of the major British participants prior to

September 1939 are dead, and none published any information;⁵⁶ the few living minor players are apparently still bound by the Official Secrets Act, as they have provided little information on that period.

This leaves two general categories of published material from the British perspective. One is the memoirs of those who were involved with Enigma at B.P. subsequent to 1 September 1939. They provide highly accurate and useful information on British operations during the war years but tend to hazard uneducated and frequently biased guesses concerning events prior to 1 September 1939. Of those who fall into this category, only F.W. Winterbotham was a professional military intelligence officer prior to the war, and he was not involved with cryptology.⁵⁷

The other category really consists entirely of a small part of one book: Appendix I to the first volume of F.H. Hinsley's three-volume study of the effect of British Intelligence on Strategy and Operations in World War II.⁵⁸ This nine-page Appendix purports to finally clarify the relative Polish, French, and British contributions to the breaking of Enigma. Since Hinsley, who had the same background of wartime work at B.P. as the other British writers, also had the unique additional advantage of access to all official intelligence files, including those which have not been and will not be released to the public, one might expect that his work would be the definitive analysis on this facet

of Enigma/Ultra. Unfortunately, however, it is rife with errors and distortions relating to material in the public domain,⁵⁹ which makes it very difficult to lean comfortably on his analysis of probably sketchy records⁶⁰ which are not available for one to check.

Thus, Hinsley's interpretations of the facts available to him must be viewed with considerable caution. He does, however, provide a few bits of information not available elsewhere that help give a general appreciation of the nature of the British efforts against Enigma in the 1930's. He confirms that pre-war records show that the French gave some documents to British Intelligence in the early 1930's - presumably Bertrand's Asche material - and notes that British Intelligence was apparently not particularly interested.⁶¹

Whatever the size of the British effort against Enigma, by 1938 the bits of information available suggest that the British had made little or no progress toward a solution, although they possessed the same materials the Poles had used to break Enigma, i.e., the Asche papers and a commercial Enigma.⁶² There must have been some serious attention given to the Enigma problem by 1936, since Hinsley notes that in that year the British, who were having some success against non-German Enigmas in the Spanish Civil War, requested further information from the French.⁶³

The Anschluss in March 1938, and the Munich Pact in September 1938, seem to have awakened the British government

to the potential threat from Nazi Germany, and provided the necessary governmental support for a greater intelligence effort against Germany, and for greater cooperation with France and Poland in various areas of intelligence. Prior to March 1938, the British Intelligence world view probably tended to see things in terms of British or non-British. The events of March and September 1938 probably either created or legitimized a perception and consequent sense that Germany was an enemy and Poland and France allies. Therefore, Bertrand's proposal of a three-way meeting in Paris in January 1939 to discuss the Enigma problem was probably welcomed by a reoriented British Intelligence Service that now saw the Enigma problem as one of far greater urgency than before.

E. THE PICTURE THROUGH 1938

Except for France's willingness as early as 1932 to share the Asche documents with other countries, during peacetime and without requiring an immediate return on this "investment," (behavior which may well be unique in the history of intelligence) the counter-Enigma picture through 1938 is essentially one of three totally separate efforts.

Since the French action in sharing the Asche material on an initiative basis is so contrary to the typical behavior of intelligence organizations, or governments for that matter, it is quite possible that Bertrand's contention, that this

was the result of his personal initiative, and that he received only grudging permission to act independently in this matter, may well be true.

Although all three of the countries involved had essentially the same assets in the early stages of attacking Enigma - some highly skilled and experienced cryptologists from World War I, a commercial Enigma machine, and the Asche material - only Poland was able to solve Enigma during this period. It may have been Poland's greater perception of danger that caused the radical decision to recruit young, inexperienced cryptologists to work on this new problem which had already defeated the experienced cryptologists. And one may speculate that these fresh minds were able to succeed where wiser heads had failed at least partly because they didn't know what any experienced cryptologist of that time could have told them: Enigma was impossible to break. Not knowing the problem was insoluble, they solved it.

Due to the changes the Germans introduced in 1938, however, the Poles were now in the same boat as the French and the British, except that they knew Enigma could be broken, and had considerable reason to feel confident that they would find a solution to these changes, as they had to the system itself in 1932.

CHAPTER III
END NOTES

1. Lewin, p. 3.
2. Ibid., p. 4. Lewin quotes from the report of a Dutch Army Captain on a two-month test performed on Enigma in 1926-1927: "Being an expert in ciphering and deciphering matters I don't shrink back from saying that even the possession of an equal machine with the same electrical connections both in the ciphering cylinders and in the other parts of the machine will not enable an unauthorized person, though he may be an expert in deciphering, to decipher a certain document or to find out its solution by scientific methods, unless he knows the whole key...".
3. Gwido Langer, Report for 1939-40, appendix: France (Paris: 12 May 1940).
4. Marian Rejewski, "Remarks on Appendix 1 to British Intelligence in the Second World War by F.H. Hinsley," trans. Christopher Kasperek, Cryptologia, VI, 1 (January 1982), p. 81.
5. Besides his unpublished reminiscences written in 1967, Rejewski has shared his memories with scholars and historians quite freely in the years since the Enigma matter became public knowledge. A particularly rich source of material from Rejewski in English is the January 1982 issue of Cryptologia cited above, which contains several articles and conversations with him.
6. Stefan Mayer, "The breaking up of the German ciphering machine Enigma by the cryptological section in the 2-nd Department of the Polish Armed Forces General Staff" (London: 31 May 1974).
Stefan Mayer, "Supplement to the paper of 31.5.74: "The breaking up of the German ciphering machine Enigma" (London: 4 December 1974).
These two papers were consulted in researching this paper through the kindness of Dr. Richard A. Woytak and the Pilsudski Institute, New York.
7. Mayer, May 1974, p. 9.
8. Gwido Langer, "Wyniki pracy: dane dotyczace depesz szyfrowych "Enigma" 6.VII.1939 - 21.VI.1940" ("Summary Data Concerning Deciphered "Enigma" Messages 6 July 1939 - 21 June 1940"). An unpublished five-page list of Enigma

cipher days broken and the dates they were read. The report covers June 1940, so may not be the same report cited in Note 3 above, which was apparently written in May 1940.

9. Gwido Langer, Reminiscences (England: 1946).
10. Richard A. Woytak, On the Border of War and Peace: Polish Intelligence and Diplomacy in 1937-1939 and the Origins of the Ultra Secret, East European Monographs, No. XLIX (Boulder, Colorado: East European Quarterly, 1979), pp. 1-4.
11. Stefan Korbonski, "The True Story of Enigma - The German Code Machine in World War II," East European Quarterly, XI, 2 (Summer, 1977), p. 228.
12. Woytak, On the Border of War and Peace, pp. 2-3.
13. Ibid.
14. Korbonski, p. 228: "...by deciphering German messages the Polish experts informed their government of the secret Soviet-German military agreement which the Germans signed in violation of the 1919 Versailles Treaty...".
15. Richard A. Woytak, "The Origins of the Ultra-Secret Code in Poland, 1937-1938," The Polish Review, XXIII, 3 (1978), p. 80.
16. Lewin, p. 7.
17. Mayer, May 1974, p. 1.
18. Richard A. Woytak, "A Conversation with Marian Rejewski," trans. Christopher Kasperek, Cryptologia, VI, 1 (January 1982), p. 50.
19. Woytak, "Conversation," pp. 52-53.
20. Bertrand gave the dates in his book (p. 37) as 7-11 December 1931. Rejewski notes elsewhere (Woytak, "Conversation," p. 54) that he corresponded with Bertrand on this point, and Bertrand acknowledged that the date should have been December 1932.
21. Woytak, "Conversation," p. 54.
22. Mayer, May 1974, pp. 2-3.

23. In fact, Bertrand states specifically (p.37) that Langer promised to keep him informed of results obtained ("il me promet de me tenir sans cesse au courant des resultats obtenus").
24. Bertrand, p. 39.
25. Ibid., p. 42.
26. Ibid., p. 39.
27. Garlinski, p. 41.
28. Marian Rejewski, "Mathematical Solution of the Enigma Cipher," trans. Christopher Kasperek, Cryptologia, VI, 1 (January 1982), p. 17.
29. Rejewski, "Mathematical Solution...", pp. 15-16.
30. Rejewski, "Remarks on Appendix 1...", p. 80.
31. Paul Paillole, Services Speciaux (1939-1945) (Paris: Robert Laffont, 1975).
32. Henri Navarre, Le Service de Renseignements 1871-1944 (Paris: Librairie Plon, 1978).
33. Interview with officials of the French Army Historical Service, Paris, Chateau de Vincennes, 6 January 1983.
34. Bertrand, p. 100.
35. Ibid., pp. 138-139.
36. Ibid., p. 227.
37. Pierre Renault, "La machine a chiffrer "Enigma"," Bulletin Trimestriel de l'Association des Amis de l'Ecole Superieure de Guerre, No. 78 (2d trimestre 1978). General Renault disapproves, for example, of Bertrand's tolerant attitude (Bertrand, p. 105) toward the British attack in 1940 on the French fleet at Mers-el-Kebir (Renault, p. 56).
38. Bertrand, p. 14 ("le veritable et "seul" artisan de cette Enigme").
39. Several authors, including Bertrand, mention a Captain Henri Bracquenie as attending the July 1939 meeting in Warsaw with Bertrand, and note that Bracquenie was a cryptologist, whereas Bertrand was not, but none ascribes any substantial role in the Enigma affair to Bracquenie.

40. Some samples of Lewin's remarks: "...he was no cryptologist; he was vain and self-seeking" (p. 15). "Bertrand was not an attractive personality" (p. 16). Lewin is also horrified that Bertrand in his memoirs "printed in full the citations for the decorations received not only by himself, but also by his wife" (p.15) (*italics his*), neglecting to note that in 1973 this was the only even slightly official documentation available to support his story. Lewin apparently sees no irony in his negative reaction to Bertrand's citations (listed at the end of the text) compared with his approbation of Winterbotham who, in accordance with British custom, one presumes, includes his CBE (without citation, it is true) on the title page of his book.
41. Bertrand does not specifically state that the Asche documents were given to the British during his visit in the early 1930's, but the fact that they were conveyed is confirmed in F.H. Hinsley, E.E. Thomas, C.F.G. Ransom, and R.C. Knight, British Intelligence in the Second World War: Its Influence on Strategy and Operations, Appendix 1, I (London: Her Majesty's Stationery Office, 1979), p. 488: "GC and CS records...confirm that the French provided GC and CS (they say as early as 1931) with two photographed documents giving directions for setting and using the Enigma machine Mark I which the Germans introduced in 1930. They also indicate that GC and CS showed no great interest in collaborating..."
42. Bertrand, p. 18.
43. Ibid., pp. 18, 20.
44. Ibid., p. 23 ("la mariee est trop belle").
45. Ibid., p. 24. There has been some confusion concerning Bertrand's designation of the agent as "Asche" and other references to an agent code-named "HE," which is phonetically identical to "Asche" when pronounced in French. Henri Navarre clarifies this point (p. 70, footnote) by noting that HE was the agent's code name in his work for Navarre's section, and the code name Asche was reserved for his work regarding ciphers, especially Enigma ciphers, for Bertrand's section. It was apparently a bit like a person with two part-time jobs: each company assigns its own personnel identification number.
46. Renauld, pp. 44, 53.
47. Bertrand, p. 25.

48. Ibid., pp. 29,32. Hinsley, among other errors, directly distorts Bertrand's statement about the Asche documents. Hinsley states (p. 488): "From Asche, according to Bertrand, the French obtained no less than 303 documents graded Geheim or Geheime Kommandosache about the Enigma." In fact, Bertrand states (p. 29) that he received 303 documents from Asche on the German CIPHERING Office, and then (pp. 30-35) groups these documents into categories, with only 16 specifically given (p. 32) as relating to Enigma.
49. Ibid., pp. 36-41.
50. Ibid., pp. 37-41. Bertrand notes (p. 39) that the Latvian visit was to a French Intelligence Service interception site functioning there with the agreement of the Latvian General Staff, not to a Latvian intelligence organization. Therefore, Latvia per se was not a party to the Enigma matter.
51. Ibid., p. 38; Hinsley, p. 488.
52. Bertrand, p. 57.
53. Lewin, pp. 20-21.
54. Bertrand, pp. 56-58.
55. Winterbotham, p. 5.
56. Steward Menzies, who was Deputy and then Chief of MI-6 before and during the war, apparently did write his autobiography prior to his death in 1968, but it is held in MI-6 files and seems not to be intended for publication. (Peter Hennessy, "Disclosures 'would have horrified MI6 chief'," The Times (London), 1 June 1977, p. 2).
57. Some of the others are cited elsewhere in this paper (e.g., Calvocoressi, Lewin, Welchman). Their works are excellent recollections of the work performed at Bletchley Park, but their grasp of matters prior to their arrival at B.P., and sometimes of matters outside their purview or experience, frequently ranges from sketchy to credulous.
58. See Note 41 above.
59. See, for example, Note 41 above for his distortion of Bertrand's statement concerning the Asche documents, and pp. 64-65 below for his trivializing of the Polish role in the Enigma affair.

60. Hinsley, p. 488: "GC and CS records are far from perfect for the pre-war years."
61. Ibid.
62. P.F.G. Twinn, Letter to the Editor, The Times (London), 21 October 1977, p. 15. Twinn notes in his letter that "With the deaths of Dilwyn Knox, Professor A.M. Turing and F.A. Kendrick, I think I am the only live British cryptographer to have worked on the Enigma machine both before and during the war...[T]he principles of this machine were fully comprehended by me and my colleagues before the war, if for no other reason than that we possessed a simple commercial version of the machine."
63. Hinsley, p. 488.

IV. THE THREADS CROSS (JANUARY-AUGUST 1939)

A. THE PARIS MEETING (9-11 JANUARY 1939)

The attendees at the Paris meeting included Langer and Ciezki for Poland, Bertrand and an unnamed cryptologist for France, and Denniston and two unnamed cryptologists for Great Britain.¹ None could read Enigma-based ciphers at that time. They left the meeting with no more knowledge than when they arrived, except for an acquaintance with their "opposite numbers" in the cryptology sections of the other countries. A brief review of the positions and probable instructions that the attendees had for this meeting makes obvious the reasons for its failure.

-The Polish contingent had the most information to give but, according to Col. Mayer, they had instructions not to divulge anything about the Polish success with Enigma unless the others present had something to offer in return.² In other words, the Poles, with some six years of successful breaking of Enigma behind them, were concerned but not yet desperate about their failure to solve the September 1938 changes. Having achieved the impossible in 1932, they probably believed they could do it again. They were in Paris essentially to pick up whatever they could from the others to help them do it faster, not for the purpose of contributing their knowledge to bailing out the others.

-The British also were probably there to see what anyone else knew that might contribute to the British efforts, rather than to share any information or insights they may have had. This may seem a leap of logic, since it has been stated previously that no information is available on British cryptologic efforts or policies prior to 1 September 1939. This opinion is based on a single nugget of information in Hinsley's study: British Intelligence was prohibited by government regulation from exchanging cryptologic information with the French as late as April 1939.³ Therefore, even if British Intelligence had made some progress in breaking Enigma, of which we remain unaware, the British attendees at the Paris meeting would have been prohibited from sharing it with the others present. They must, therefore, have attended to find out what the French and the Poles might know what the British could use.

-The French, of course, were quite obviously there to acquire information, since Bertrand had been quite open with the others concerning his organization's lack of success against Enigma. Judging by his previous action in giving the Asche documents to the Poles and the British, it seems likely that he would have revealed any information he had.

The make-up of the national contingents is also evidence that each organization saw the meeting as a quid pro quo occasion. In each case, the officers sent were Chiefs rather than Indians. The British and Polish attendees had backgrounds

as working cryptologists but, as one can verify in the Polish case, at least, did not include any of those who actually broke Enigma. They were probably expert enough on the problem to recognize information worth acquiring when they heard it, but probably not sufficiently familiar with the nitty-gritty details to usefully engage in working-level analytical discussions of the ins and outs of deciphering Enigma messages. They were there as information negotiators, not technicians.

On the other hand, the prior and subsequent positions of these Polish, French, and British officers in their countries' cryptologic organizations, and their centrality to pre-war and wartime counter-Enigma operations, indicates that the Paris meeting and the breaking of Enigma were taken seriously by all of the countries involved. The difficulty was that, to begin the flow of information at that meeting, someone needed to prime the pump, and everyone there was either unwilling or unable to make the first move.

The result of the meeting, then, was a platitude about sharing any progress each might make, keeping in touch with each other on this problem, and calling another meeting should any of the attendees feel that some new development warranted one.⁴

B. BUSINESS AS USUAL (FEBRUARY-JUNE 1939)

Subsequent to the January 1939 meeting in Paris, all three countries appear to have continued their efforts separately

until July 1939. After the Czechoslovakian occupation, the British apparently changed their regulations to permit closer cryptologic cooperation with the French,⁵ at least, but there are no indications that this resulted in any significant differences in the level of cooperation. Then again, Hinsley refers to the regulations concerning the French only; if a change to the regulations did not include the Poles, it would have had little impact on the Enigma problem, since neither the British nor the French apparently had anything to exchange in that area.

Col. Mayer stated that a decision had been made that, "in case of a threat of war the Enigma secret must be used as our Polish contribution to the common cause of defence and divulged to our future allies."⁶

It is worth noting that the gift was probably not intended to be without strings. Most French and British writers today seem to be conveniently confused by 20-20 hindsight into perceiving Poland's gift as a gallant gesture from one who can foresee his imminent demise - sort of a "morituri te salutamus." In view of the subsequent events, it seems have been assumed that Poland's speedy defeat by Germany was known to be inevitable. It is conveniently forgotten that Poland believed itself to be well and truly bound by treaty to two allies - Great Britain and France - who would join Poland in its defense against an invader. The Poles seriously expected to see British and French planes in the air over Warsaw after

1 September 1939. The gift in July 1939 should be seen as an acknowledgement that war was inevitable and probably imminent, not that Poland would be unaided and quickly defeated. Enigma was probably not intended to be passed on, like a torch from a falling runner, but shared with allies who could use their greater economic resources to manufacture deciphering aids to overcome the September and December 1938 changes and thus enable all three allies to better defend Poland in the event of a German attack.

C. THE WARSAW MEETING (24-25 JULY 1939)

Whatever the motivations, the meeting in Warsaw was called by the Poles to reveal the extent of their success to the French and British attendees. It was attended by Bertrand and Henri Bracqueniet for France; Denniston, Knox, and a mysterious "Professor Sandwich" for Great Britain; and Mayer, Langer, Ciezki, Rejewski, Zygalski, and Roczycki for Poland. The first day was apparently taken up with arriving, settling in, and having a luncheon. The next day the visitors were taken to the Polish cryptologic unit's headquarters in the Pyry Forest, and the full extent of the Polish success - and recent failure - was revealed. Arrangements were made to ship two Enigmas and related sets of technical drawings (for bombes and perforated sheets) to Paris via diplomatic bag, with one machine and set of drawings to be forwarded to London. This part of the story was completed on 16 August 1939 when

Bertrand delivered the British portion of the "treasure" to London.⁷

On that date, then, the three allies were generally on the same footing, except for the much greater familiarity the Poles had with Enigma, after deciphering its messages for six years.

D. ANOTHER STORY

The meeting described above is now generally accepted as the way the French and British acquired the details of the brilliant Polish work against Enigma. The first British book published on Enigma, Winterbotham's The Ultra Secret, told a different story, however, one which has turned up in several later books and seems to be the version destined to be enshrined in fiction.⁸ Although the "Winterbotham story" does not represent the mainstream of Enigma developments, it has become popular enough to warrant some discussion. In brief, the "Winterbotham story" follows.

A Polish worker employed at a factory in Germany making Enigma cipher machines was sacked sometime in the 1930's, and returned to Poland, where he contacted British Intelligence with an offer to tell them everything he knew about the then-mysterious German cipher machine. British Intelligence persuaded him to go to Paris, where, after the Deuxieme Bureau helped set him up in a workshop, he constructed a large model of the machine he had worked on. With the model

to help them identify it, British Intelligence determined that it was a modification of the commercially-available Enigma machine. Believing that it would be necessary to have one of the modified Enigma machines in hand in order to break its ciphers, British Intelligence gave Polish Intelligence the necessary money and Polish Intelligence "acquired" a machine, by means not specified. Then, "it was Denniston himself who went to Poland and triumphantly, but in the utmost secrecy, brought back the complete, new, electrically operated Enigma machine" to England. The British then set to work, invented a machine called the "Bronze Goddess" (like a bombe?) to help, and, by April 1940, had broken the first Enigma-based cipher.⁹

Winterbotham's book appeared in London on 23 October 1974.¹⁰ On 3 November 1974, the first outraged denial by those aware of Polish and French efforts appeared in the London Times.¹¹ Winterbotham then inserted the following paragraph in the first U.S. edition, which appeared shortly thereafter:

Since this book was completed, Polish officers now living in Britain have stated that the Poles constructed a number of Enigma machines from information extracted from the factory in Germany coupled with the help of their own cryptographers, and that it was presumably one of these which they supplied to us. This may very well be true and certainly the Polish mathematicians and technicians displayed brilliance and great courage, but the story I have given is the one told to me at the time.¹²

There would appear three options for evaluating this story:

--Winterbotham may have invented it out of whole cloth, either to avoid revealing anything about "sources and methods" by which Enigma was broken, or simply to reserve all credit to the British, or for some other unknown reason;

--The story may have no basis in fact, but still have been the story Winterbotham was told at the time, possibly because he had no "need-to-know" the "sources-and-methods" involved;

--The events Winterbotham described may have occurred largely as stated, which would not necessarily contradict the other story: that is, both stories could be true.

There is probably no way of determining now which if any of these options is correct, unless additional information should become available. The difference in impact between the first and second options is negligible, in any case, but the third is a bit more intriguing.

On the face of it, the "Winterbotham story" appears to represent an alternate reality which is cancelled by the reality recounted throughout this paper. However, a closer examination reveals that they could be parts of the same reality.

The part of the "Winterbotham story" which concerns the Polish worker in Paris, for example, is of a failed attempt made when the British did not know the Poles had any success. If one ignores the implication that the Britain did not know that the Enigma machine was in question, the remainder of the

story is quite possible. It is not only logical that British Intelligence would be trying every means at its disposal, but it is to be expected.

The other part of the "Winterbotham story" is equally feasible and suggests a rather charming scenario. The Poles were aware shortly after the Germans added rotors in December 1938 that their bombes and perforated sheets would have to be remade, an expensive process that an economically impoverished Poland could not afford. How nice it would have been to have British Intelligence appear, as one is pondering how to afford this expense, and offer a substantial sum for an Enigma machine, of which there are a goodly number available, largely because they are being built right there in Warsaw. Selling British Intelligence one of the Polish Enigma copies would be a perfectly honorable transaction, benefiting both the seller and the buyer, without the buyer having any hint that the seller had been reading Enigma messages and building Enigma copies for six or seven years.

This scenario is probably a pipedream, but a rather alluring one, nonetheless. In any case, if any part of it occurred, it was overtaken by events when the Polish government decided to give all of the Enigma information to France and Great Britain in July 1939.

CHAPTER IV
END NOTES

1. Lewin, p. 20.
2. Mayer, May 1974, p. 4.
3. Hinsley, p. 488.
4. Bertrand, p. 58.
5. Hinsley, p. 488.
6. Mayer, December 1974, p. 2.
7. Garlinski, pp. 42-45.
8. Donald Freed, The Spymaster (New York: Bantam Books, 1981), pp. 50-51.
9. Winterbotham, pp. 9-16.
10. "R.A.F. Man's Book Describes Breaking of the Nazis' Codes," The New York Times, 25 October 1974, p. 2. The story is datelined London, 23 October 1974, and describes the book as "published here today."
11. Michael Pye, "Final Solution to the Enigma," The Times (London), 3 November 1974, p. 11.
12. Winterbotham, p. 16. It is worth noting that Winterbotham still managed to accord the Poles only a role as reconstructors of the machine, not as cryptanalysts, and he contrived to leave out the French altogether.

V. APRES CA, LE DELUGE (SEPTEMBER 1939 - MAY 1945)

A. THE THREADS JOIN (SEPTEMBER 1939 - JUNE 1940)

With the invasion of Poland on 1 September 1939, all of Europe changed to a war footing. After a period of non-combat known to Americans as the phony war, the fighting began again and, in June 1940, France fell. In the non-lethal war against Enigma, this period is conveniently divided into two parts: the period before Enigma was rebroken, when the intelligence services were mobilizing, organizing, and feverishly developing means of attacking Enigma, and the period when Enigma messages were read and used, though unsuccessfully, to support forces in the field.

1. The Pattern Forms (September 1939 - December 1939)

This period probably represents the most open period of cooperation among the three allies in working on the Enigma problem. Since all three were desperately trying to break back into Enigma, it was probably obvious to all that everyone had a "need-to-know" for every detail that might help toward a solution. Day-to-day communications between the French and Poles near Paris and the British in London (or B.P.) were via teletype, over which any keys identified by one side were sent to the other, as well as any other useful information.¹

There was apparently also some face-to-face discussion. Bertrand notes that he made a trip to London during this period;²

Mayer states that Langer also visited London,³ and that he himself visited Vignolles.⁴ Hinsley and others have also indicated that there was at least one British trip (by Turing) to Vignolles in December 1939.⁵

The only note of discord reported during this time is an indication that the British wanted the Poles to come to England in December 1939 (because the perforated sheets were now available?), but apparently they refused. One can easily see that the Poles would have refused. All of the Polish Army that had escaped from Poland was located in France, not England. Since the Poles regarded their primary task as one of support to Polish Intelligence, which was part of the Polish Army, not as a choice between the French and the British, it is quite logical that they would choose to remain in France, closer to their own combat forces and certainly not aware that they would be at risk because of France falling so rapidly in June 1940.

a. The Polish Needle

Poland was invaded on 1 September 1939 and defeated handily in four weeks. Even if its allies had joined in the fight, it is debatable whether the eventual outcome would have been any different; without their help, the defeat was fast. It is somewhat ironic that the country whose military intelligence organization had solved the most sophisticated system flourishing in an exotic field such as cryptology was in the position of pitting horse cavalry against tanks.

Bertrand notes that radio contact was maintained via the BLR link with Pyry Forest until 10 September 1939, which is presumably the date the facility was evacuated. The Poles took two Enigma machines with them, but destroyed everything else at Pyry Forest so thoroughly that the Germans never did discover what work had been done there.⁷

Polish Intelligence, including the cryptologic section, accompanied the government to its initial exile in Romania. Some of the cryptologists made their way to the British Embassy to seek transport to the West, but had the bad luck to arrive just as the convoy from the British Embassy in Warsaw was being processed. The Poles were told to return later, but decided to try the French Embassy first. There they were welcomed with open arms, because Bertrand had sent word to Embassy officials to be on the look-out for them and to give them every assistance in reaching France. Arrangements were made immediately and, by 1 October 1939, Langer and 14 cryptologists were in France, ready to work.⁸

Their status in France was as an operating unit of the Polish Army, most of the residue of which was gathering in France, where the next round of fighting was expected to begin soon. At no time during the war years did the Polish cryptologic unit "belong" to French Intelligence; rather, it collaborated and was colocated with the French cryptologic unit as a matter of mutual benefit. The Polish cryptologic unit was given permission by Polish authorities to integrate

their work with that of the French because Polish intercept facilities had not been evacuated from Poland, and a cryptologic unit is useless without the raw material provided by intercepted messages.⁹

During all of its time in France, this unit reported administratively to Polish Intelligence Service headquarters, i.e., Col. Mayer, in London, and operationally to both Polish and French Intelligence authorities simultaneously. The French Intelligence authority on the spot was, of course, Bertrand, who was chief of the expanded cryptologic activity located at Chateau Vignolles near Paris.

b. The French Needle

The French mobilization transformed Bertrand's probably small cryptologic unit into what Lewin has referred to as the "first allied operational intelligence center."¹⁰ It included personnel of four nationalities working for three countries in what must have been an administrative nightmare. In addition to a French team of 75 persons, and the Polish team of 15, there was a Spanish team of 7 persons, and an integrated liaison officer from Great Britain who had dedicated communications (a teletype) with London to ensure that the two halves of the Enigma operation remained in sync. The Spaniards, who were enrolled in the French Foreign Legion, were, therefore, unlike the Poles, a wholly-owned asset of France. They were the remnants of the Spanish National Government's cryptology unit, and had been salvaged by Bertrand from among the Spanish Civil War refugees in southern France.¹¹

Bertrand mentions only the Enigma work of the Polish team, so the tasks of the French and Spanish teams are uncertain. Since France had the full benefit of the Polish team's work on Enigma, it is possible that the other teams were never tasked with Enigma deciphering. The Spanish team worked on Spanish and Italian ciphers¹² and the French team may have performed other tasks, such as the analytical and evaluative function described by various British authors as done on the British side by Hut 3 at B.P.

c. The British Needle

Like the French, the British military establishment expanded to wartime strength and organization upon the German invasion of Poland. For MI-6, this included the permanent move of the cryptologic organization to Bletchley Park and the recruitment of many additional personnel.¹³ A group of scientists, mathematicians, and university professors had been "short-listed" previously for wartime cryptology duty, and these were soon augmented by additional personnel. The organization and operations of B.P. have been amply described by various British authors and will not be further discussed here.

One may assume that a great deal of attention was immediately devoted to the problem of rebreaking Enigma. The Polish Enigma and technical drawings were, of course, available. How much impact the Polish work had on the British methods of solution has been a point of great controversy.

At a minimum, in September 1939, the presence of the Polish Enigma resolved the British lack of knowledge of the internal wheel wirings.¹⁴ At a maximum, the British simply copied all of the Polish methods (expanding the aids to deal with the additional rotors). These two extremes have been well expressed by two previous commentators. The truth, as one might expect in such a complex arena, probably lies somewhere in between.

The latter position was adopted by Bertrand, though he never specifically denigrated British efforts, when he wrote:

As for the Polish cryptanalysts, to them alone goes all the credit and all the glory of having carried through to completion, technically, this incredible adventure, thanks to their skill and tenacity, unequalled in any other country in the world!¹⁵

The judgement that the Polish impact was minimal was made by Hinsley:

The Bombe greatly increased the speed and regularity with which GC and CS broke the daily-changing Enigma keys. From the summer of 1940, as more and better models were built, it was the essential basis of GC and CS's continuing and increasing success. On this account, and because GC and CS had not thought of the possibility of using high-speed machine testing against the Enigma before the July 1939 meeting, it has been argued that the Poles made their most valuable contribution by then providing the diagrams of their Bombe. But the British Bombe was of quite different design from the Polish and much more powerful; and it is virtually certain that the GC and CS Enigma team would in any case have realized the need to develop analogue machinery for recovering the daily keys as soon as it had discovered the wirings of the Enigma wheels--the more so since the team included Turing, who already had an interest in machine computation....the most important outcome of the July meeting was that the Poles handed over the results of their brilliant work in

recovering the wheel wirings, though an additional benefit--imponderable but potentially of great psychological value--was the very discovery that the Poles had had such significant success.¹⁶

Having dismissed the fact that the Poles conceived the concept of using Bombes to help recover the keys, which is a lot like saying that Einstein's theory of relativity is no credit to him, because someone else would have thought of it eventually, Hinsley removes the Poles neatly from the team playing the game and places them in the position of cheer-leaders: their only real gift "imponderable but potentially of great value--was the very discovery that the Poles had had such significant success."

While one may certainly accuse Bertrand of being somewhat biased against the doubtless brilliant British work, Hinsley appears to be distorted excessively far in the other direction.

Since there is apparently some official stricture still in effect regarding the technical apparatus and methodology used at B.P., we may never know clearly how much each group contributed to the permanent solution of Enigma, but it seems safe to say that kudos are deserved all around.

2. The Pattern Blurs (January 1940 - June 1940)

The first break into the German military Enigma since December 1938 occurred, according to three different sources, on 28 October 1939 (Bertrand);¹⁷ the latter part of December 1939 (Hinsley);¹⁸ and 17 January 1940 (Langer).¹⁹ I tend to

feel most comfortable with Langer's date as the likeliest, for several reasons.

--Langer's report was written in 1940, when the memory of that moment was quite fresh. Also, since his report lists 126 daily settings broken and the date each was broken, it was probably compiled from a log in which entries were made of events as they occurred.

--Bertrand's date is for the daily setting which Langer says was broken on 17 January 1940. Bertrand may simply have made an error.

--Hinsley's date corresponds to the time that Turing brought the set of perforated sheets on which the break was made to Paris. It is possible that, whatever the source of Hinsley's information, the date for bringing the sheets over was confused with the date they were first used successfully.²⁰

It is interesting that the break was made using perforated sheets rather than "bombes." In fact, there were as yet no bombes available, since the Poles had destroyed theirs when evacuating Warsaw, the French hadn't built any, and the British were still building theirs.

Hinsley refers to these sheets as "GC and CS punched-hole sheets,"²¹ yet the fact that they were carried to Paris and the break made by the Poles there suggests that the Poles had some expertise or familiarity with using these sheets that the British didn't have, else they would have simply used the sheets at B.P. and broken out the key themselves.

Therefore, it seems likely that these were simply a British remanufacture of the Polish perforated sheets for which technical specifications had been provided at the Warsaw meeting in July 1939. The timing of this event also suggests that the reason for the British invitation for the Poles to transfer to London in December 1939 may have been that the first set of sheets had been completed and the Poles could demonstrate them and train the British in their use.

In any event, the first break was probably made on or not too long before 17 January 1940, and the keys and settings started to tumble out more and more quickly after that first break. During January and part of February 1940, it seems to have taken about two weeks to break a key, then several days to one week until April 1940, then a couple of days during April, and, in May and June 1940, keys were being broken out the same day or the next day.²² Some of this constant acceleration may have been due to increasing familiarity with the hand methods, but most probably was related to implementation at B.P. of various mechanical aids. The shift from a two-week to a one-week delay in February 1940 is roughly congruent with Winterbotham's comment²³ that he was shown the "Bronze Goddess" - probably a Polish-type bombe? - early in 1940. Likewise, Hinsley notes that the first British-made bombe was available in May 1940,²⁴ when breaking the keys was becoming routine.

Langer's report also notes that 83% of the keys broken during this period came from B.P.²⁵ This is hardly surprising, since all of the mechanical aids were located there. There is no evidence, incidentally, that the British were discussing with the Poles or the French any of their technical advances in constructing bombs. Welchman, who was an integral part of the British team, indicated recently that he didn't know until 1981 that there was an Enigma deciphering operation in France.²⁶ This would strongly suggest that the British were working in isolation on their cryptologic effort.

The halcyon days of full cooperation were already over. The French and Polish units were probably still cooperating fully because they were physically and functionally interdependent, but the British, remotely located and functioning independently, were already favoring "need-to-know" over "common cause."

Like Poland in September 1939, France fell more quickly than anyone would have thought possible after the German attack of 10 May 1940. German advances were so quick that Vignolles was evacuated to Paris a few days after the 10 May 1940 attack. When Paris was threatened, the entire cryptologic operation moved out by bus and car toward the south, following the retreating French government. At each stop, the deciphering efforts continued, and contact was maintained by radio with London. When the armistice became inevitable, the group was dissolved. The British Liaison

Officer returned to London from Cazaux airfield, the Poles and the Spaniards were flown to Algeria from Toulouse airfield and, when the armistice arrived, French personnel were demobilized. The radio link with London ended 28 June 1940.²⁷ Britain seemed to stand alone in Europe, with the fragile protection of the English Channel and the growing ability to read a lot of Hitler's mail.

B. TANGLED THREADS (JULY 1940 - DECEMBER 1942)

This story of "needles and haystacks" would seem over at this point, with only the MI-6 needle surviving in the British haystack. The Poles and Bertrand, being nothing if not innovative, however, soon got back into the game, albeit only peripherally.

Bertrand, along with other professional French military personnel, was not demobilized with the conscripts in July 1940, but was retained on active duty as a member of the small Vichy Army permitted by the Armistice. His branch of service, as before, was intelligence and, along with quite a few other French military intelligence personnel, he was simultaneously an officer of the Vichy S.R. and of the "shadow" S.R. organization known as Réseau Kleber, which was pro-Allies and anti-Nazi. It was in this latter role, presumably, that he reconstructed his cryptologic unit (Spanish and Polish teams only) at a chateau near Nimes code-named P.C. Cadix.²⁸

While ostensibly working as a Vichy communications security organization, P.C. Cadix began deciphering Enigma

and other signals traffic and, in March 1941, reestablished direct communications with London (MI-6) via clandestine radio.²⁹ During this time, then, Bertrand was personally operating in four roles: responsible to Vichy for the overt work of his unit; responsible to Réseau Kleber (and thence to Giraudists in Algiers) for clandestine signals intelligence on the Germans; responsible to London (and thence to B.P.) for contributions to Enigma and other deciphering activities; and responsible otherwise to MI-6 for agent intelligence.

He made some 100 trips across the demarcation line to German-occupied Paris. Most of these were as a Resistance agent of MI-6 and Réseau Kleber, to contact a source he had developed at the German Embassy.³⁰ Some, however, were related to Enigma operations.

During the phony war orders had been placed with a Paris manufacturing concern for various parts of Enigma machines, based on the Polish specifications provided in July 1939. Since the parts had not been received prior to the fall of France in June 1940, Bertrand made 26 trips to Paris to pick up Enigma parts, which the Poles assembled into four additional Enigma machines at P.C. Cadix.³¹

The situation of the Polish team during this time was even more complicated than Bertrand's. Langer and his subordinates returned to France in October 1940 with the approval of Polish Intelligence authorities in Algiers and London. Once again they were working hand-in-glove with

Bertrand and French Intelligence but, as before the fall of France, they were subordinated to Polish Intelligence.³²

So, while Bertrand was communicating with MI-6 in two of his roles, at least part of the time using a one-time-pad cipher which could not even be read by anyone else at Cadix, the Poles were communicating with Polish Intelligence headquarters in London, over the same radio,³³ but using their own cipher, which Bertrand couldn't read. They also operated as part of Bertrand's roles in providing signals intelligence to MI-6 for B.P., to Vichy, and to Réseau Kleber. This makes them even with Bertrand with four roles each, but the Poles went Bertrand one better.

The only restriction the "men of good will" at Vichy who knew about Réseau Kleber had placed on Bertrand's (and, presumably, Réseau Kleber's) connection with MI-6 was that no information about Vichy itself be passed. The Poles solved that problem by passing intelligence on Vichy directly by radio to a Polish intelligence network in Algeria called the Rygor Network, supposedly without Bertrand's knowledge.³⁴

This situation continued until early November 1942, when the German occupation of the Vichy Zone in reaction to the Allied landings in North Africa put a stop to French and Polish participation in the Enigma saga. By the end of 1942, Bertrand and his wife had temporarily gone to ground on the Riviera, the Spaniards had been evacuated, and the Poles were attempting to escape to Spain and then Britain via the Pyrenees.³⁵

C. THE ENDS (JANUARY 1943 - MAY 1945)

Having followed Bertrand and the Poles through their peripatetic pre-war and wartime search for Enigma, one cannot simply leave them in hiding in southern France.

Bertrand continued to function as part of Reseau Kleber until January 1944 when, on his 101st trip to Paris since the fall of France, he was arrested by the notorious Masuy, a French collaborator with the Abwehr. During his questioning he was told that the Germans had arrested and shot Asche, and had Lemoine in custody. They apparently knew that Asche had sold the French some cipher documents, but still believed that Enigma was unbreakable. Bertrand convinced Masuy and company that he would be willing to turn Reseau Kleber against the Allies, and then went into hiding until May 1944, when he was lifted out of France by an MI-6 network, arriving in London just two days before D-Day.³⁶ Bertrand was then Chief of Intelligence to General Koenig's French Forces of the Interior, which was by this time an Allied organization coordinating all Resistance activities during Allied advances in France.³⁷ Bertrand and his wife returned to France in September 1944³⁸ and, according to Bertrand, he recovered Enigma machines and files at P.C. Cadix and began operating again in January 1945, continuing until the end of the war.³⁹

Some of the Poles, including Rejewski and Zygalski,⁴⁰ escaped over the Pyrenees in early 1943, and went on to London. They were not permitted at Bletchley Park, but worked with a

Polish Signals Intelligence Unit near London on non-Enigma ciphers.

Langer, Ciezki, and three other Poles were captured by the Germans while trying to escape over the Pyrenees. They spent the remainder of the war as prisoners. Langer and Ciezki survived, but two of the others died.⁴¹

The threads ended, then, as separately as they had begun: each group of cryptologists was completely isolated from the others. The security consciousness (bordering on paranoia) which is typical of intelligence organizations had regained the ascendancy, with the "family jewels" now in British possession rather than Polish. The British, of course, went on to make the counter-Enigma operation into Ultra - an achievement of interception, deciphering, analysis, and dissemination on a scale that probably would have astounded the Polish and French pioneers, who were never permitted to visit B.P. or know of its achievements.

CHAPTER V
END NOTES

1. Wldyslaw Kozaczuk, "Enigma Solved, "Cryptologia, VI, 1 (January 1982), p. 32. Kozaczuk reports on a conversation he had in 1975 with Henri Bracquenie, who was responsible for establishing the procedures for these information exchanges. Bracquenie informed him that Enigma machines were used to encipher these communications!
2. Bertrand, p. 76.
3. Mayer, May 1974, p. 5.
4. Mayer, December 1974, p. 4.
5. Hinsley, p. 493.
6. Christopher Kasperek and Richard A. Woytak, "In Memoriam Marian Rejewski," Cryptologia, VI, 1 (January 1982), p. 21.
7. Bertrand, p. 69.
8. Kasperek and Woytak, "In Memoriam...", p. 21.
9. Mayer, May 1974, p. 4.
10. Lewin, p. 31.
11. Bertrand, pp. 70-72.
12. Ibid., p. 71.
13. Calvocoressi, pp. 12-13.
14. Twinn notes: "The wartime problem was first, to reconstruct the particular internal connexions used by the Germans and, secondly, to deduce the daily settings."
15. Bertrand, p. 61.
16. Hinsley, p. 494.
17. Bertrand, p. 76.
18. Hinsley, p. 493.
19. Langer, p. 1.

20. Oddly enough, Hinsley, who states firmly (p. 493) that "an Army Enigma key (the key named the Green at GC and CS) for 28 October was broken in the second half of December," seems to contradict himself in the second volume of his three-volume work. In Appendix 4 ("Enigma Keys Attacked by GC and CS up to mid-1943") to the second volume, he lists (p.662) German Army Enigma Key "Green" as having been broken on 18 January 1940.
21. Hinsley, p. 494.
22. Langer, pp. 1-5.
23. Winterbotham, p. 15.
24. Hinsley, p. 494.
25. Langer, p. 5.
26. Welchman, p. 17.
27. Bertrand, pp. 100-103.
28. Ibid., pp. 107, 109-110.
29. Ibid., pp. 110-111.
30. Ibid., pp. 111-112. Hinsley notes Bertrand's contributions to MI-6 as a source of agent intelligence in several places (pp. 94, 130, 474, 701) in Volume II of his study of British Intelligence during the war.
31. Ibid., p. 111.
32. Mayer, May 1974, p. 7.
33. Ibid., May 1974, p. 7.
34. Ibid., May 1974, p. 7.
35. Bertrand, pp. 140-143.
36. Ibid., pp. 158-204.
37. Ibid., pp. 215-216.
38. Ibid., p. 223.
39. Ibid., pp. 227-228.

40. Roczyki had died in 1942 when the ship which he was returning from Algiers was sunk (Bertrand, p. 124).
41. Mayer, May 1974, p. 8.

VI. CONCLUSIONS

Anyone who has come this far through the Enigma-tic maze is entitled to wonder what interest it may have for a reader or, for that matter, a writer 40 or 50 years later. Should it be perceived as a historical puzzle that, much like a detective story, is satisfying simply to unravel? Could it be viewed primarily as an adventure story, filled as it is with secret codes, brave heroes, wily spies, undercover Resistance organizations, and lots of doubling and tripling of various intelligence organizations? Or, might one find in this story useful lessons for today, in the same way that it has become fashionable for books on wartime Enigma/Ultra operations to focus on the impact the Ultra decrypts had on the conduct of the war?

Certainly, the story functions well as a historical puzzle. Since most of the literature in English on Enigma/Ultra to date has concerned the operations of Bletchley Park in the war years, and virtually all has described events from a single perspective, the research for this paper was a bit like detective work. Small clues to the contacts among the three intelligence services involved led to wholly unsuspected areas of information, such as the quadruple- and quintuple-hatting of the French and Polish members of P.C. Cadix.

The heroic adventure content of the story must also be acknowledged, particularly in the French and Polish operations

in Vichy France, which rival tales of James Bond for danger, intrigue, and derring-do. Bertrand's experiences alone have been described by a British authority on World War II Resistance as a classic case history of what a truly professional intelligence officer can accomplish under incredibly adverse conditions,¹ a point worth highlighting for those who prefer to consider that the debacle of the Battle of France represented the totality of French capabilities in World War II.

And, for those who expect to learn something useful from every story, a tentative moral can be drawn from this one: some of the countries involved, by adhering strictly to the "need-to-know" and "sources-and-methods" principles in the 1930's, put all of the Allies in a worse position in 1939 than they would have been had the needs of "common cause" been given more attention sooner.

For Poland, World War II brought total defeat and apparently permanent submergence in the Soviet bloc. For France, the war brought shocking military defeat and five years of humiliating occupation by a foreign power. And for Great Britain, it was five years of a harrowing and costly razor's edge. For all three and for the other countries involved on both sides, World War II represented a huge cost in human life and property.

But--what if the Poles had informed Bertrand and the French of their success against Enigma in 1933 instead of 1939? What if the British had been more interested in collaborating with

the French and the Poles in 1932 instead of 1939? Since the Poles were reading Enigma traffic freely during most of the 1930's, one can assume that the British and the French would have been, too. With the solid high-level intelligence provided by Enigma to back up their warnings, would the Western intelligence organizations have been better able to convince their governments of German rearmament and Nazi intentions? If so, would the governments still have persisted so long in their appeasement policies, or might a harder line have been adopted sooner?

The events which led to World War II are far too complex to speculate on the specific effects early access to Enigma decrypts might have had, but this thesis posits that the Allies would have been in some way, even if only marginally, better prepared.

CHAPTER VI
END NOTES

1. M.R.D. Foot, Resistance: European Resistance to Nazism 1940-1945 (New York: McGraw-Hill, 1977), p. 243.

BIBLIOGRAPHY

BOOKS

- Beesly, Patrick. Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Centre 1939-1945. New York: Ballantine Books, 1981.
- Bertrand, Gustave. Enigma ou la plus grande énigme de la guerre 1939-1945. Paris: Plon, 1973.
- Brown, Anthony Cave. Bodyguard of Lies. New York: Harper and Row, 1975.
- Calvocoressi, Peter. Top Secret Ultra. New York: Ballantine Books, 1981.
- Dille, John. TIME Capsule/1939: A History of the Year Condensed from the Pages of TIME. New York: TIME-LIFE Books, 1968.
- Dille, John. TIME Capsule/1940: A History of the Year Condensed from the Pages of TIME. New York: TIME-LIFE Books, 1968.
- Dille, John. TIME Capsule/1941: A History of the Year Condensed from the Pages of TIME. New York: TIME-LIFE Books, 1967.
- Foot, M.R.D. Resistance: European Resistance to Nazism 1940-1945. New York: McGraw-Hill, 1977.
- Freed, Donald. The Spymaster. New York: Bantam Books, 1981.
- Garliński, Józef. Intercept: The Enigma War. London: J.M. Dent & Sons, Ltd., 1979.
- Goralski, Robert. World War II Almanac 1931-1945: A Political and Military Record. New York: G.P. Putnam's Sons, 1981.
- Haldane, R.A. The Hidden War. New York: St. Martin's Press, 1978.
- Hinsley, F.H., E.E. Thomas, C.F.G. Ransom, and R.C. Knight. British Intelligence in the Second World War: Its Influence on Strategy and Operations. 2 vols. London: Her Majesty's Stationery Office, 1979-1981.

Johnson, Brian. The Secret War. London: The British Broadcasting Corporation, 1978.

Jones, R.V. The Wizard War: British Scientific Intelligence 1939-1945. New York: Coward, McCann and Geoghegan, Inc., 1978.

Kahn, David. The Codebreakers: The Story of Secret Writing. New York: The Macmillan Company, 1967.

Kahn, David. Hitler's Spies: German Military Intelligence in World War II. New York: Macmillan Publishing Co., Inc., 1978.

Lewin, Ronald. The American Magic: Codes, Ciphers and the Defeat of Japan. New York: Farrar, Straus, Giroux, 1982.

Lewin, Ronald. Ultra Goes to War: The First Account of World War II's Greatest Secret Based on Official Documents. New York: Pocket Books, 1980.

Murphy, Robert. Diplomat Among Warriors. New York: Pyramid Books, 1965.

Navarre, Henri, et un groupe d'anciens membres du SR. Le Service de Renseignements 1871-1944. Paris: Plon, 1978.

Paillole, Paul. Services Spéciaux (1935-1945). Paris: Robert Laffont, 1975.

Rock, William R. British Appeasement in the 1930's. New York: W. W. Norton & Company, Inc., 1977.

Rothschild, Joseph. East Central Europe between the Two World Wars. Vol. IX, A History of East Central Europe. Seattle: University of Washington Press, 1974.

Schoenbrun, David. Soldiers of the Night: The Story of the French Resistance. New York: New American Library, 1980.

Shachtman, Tom. The Phony War 1939-1940. New York: Harper and Row, 1982.

Welchman, Gordon. The Hut Six Story: Breaking the Enigma Codes. New York: McGraw-Hill, 1982.

Winterbotham, F.W. The Ultra Secret. New York: Harper and Row, 1974.

Woytak, Richard A. On the Border of War and Peace: Polish Intelligence and Diplomacy in 1937-1939 and the Origins of the Ultra Secret. No. XLIX, East European Monographs. Boulder, Colorado: East European Quarterly, 1979.

ARTICLES

Beesly, Patrick. Letter to the Editor, The Times [London], 22 April 1977, p. 19.

"British Tell How They Learned Nazi Secrets," The New York Times, 10 November 1974, p. 3.

Calvocoressi, Peter. Letter to the Editor, The Times [London], 29 April 1977, p. 17.

Calvocoressi, Peter. "The Ultra Secrets of Station X," The Times [London], 24 November 1974, pp. 33, 34.

Deutsch, Dr. Harold C. "The Historical Impact of Revealing the Ultra Secret," Parameters, Journal of the U.S. Army War College, VII, 3 (1977), pp. 16-32.

Deutsch, Dr. Harold C. "The Influence of Ultra on World War II," Parameters, Journal of the U.S. Army War College, VIII, 4 (December 1978), pp. 2-15.

Garliński, Józef. Letter to the Editor, The Times [London], 29 October 1977, p. 15.

Hennessy, Peter. "Disclosure of British war secrets allowed," The Times [London], 10 May 1977, pp. 1, 2.

Hennessy, Peter. "History will be changed by Enigma disclosures," The Times [London], 13 October 1977, pp. 1, 2, 16.

Kahn, David. "Le Rôle du decryptage et du renseignement dans la stratégie et la tactique des Alliés," Revue d'histoire de la deuxième guerre mondiale, Vol. 28, No. 111 (July 1978), pp. 73-85.

Kahn, David. "The Ultra Secret." Review of F.W. Winterbotham, The Ultra Secret (Harper and Row). The New York Times Book Review, 29 December 1974, p. 5.

Kahn, David. "Why Germany Lost the code War," Cryptologia, VI, 1 (January 1982), pp. 26-31.

Kasperek, Christopher and Richard A. Woytak. "In Memoriam Marian Rejewski," Cryptologia, VI, 1 (January 1982), pp. 19-25.

Korbonski, Stefan. "The True Story of Enigma - The German Code Machine in World War II," East European Quarterly, Vol. XI, No. 2 (Summer 1977), pp. 227-234.

Kozaczuk, Władysław. "Enigma Solved," trans. Christopher Kasperek, Cryptologia, VI, (January 1982), pp. 32-33.

Middleton, Drew. "WWII Stories." Review of Ronald Lewin, Ultra Goes to War (McGraw-Hill), and James Leasor, Boarding Party (Houghton-Mifflin), and Joseph Persico, Piercing the Reich (The Viking Press). The New York Times Book Review, 18 February 1979, pp. 10, 11.

Montagu, Ewen E.S. Letter to the Editor, The Times [London], 18 October 1977, p. 17.

"Now French Claim their spy found the code secret that beat Hitler," The Times [London], 27 June 1976, p. 3.

Pye, Michael. "Final Solution to the Enigma," The Times [London], 3 November 1974, p. 11.

"R.A.F. Man's Book Describes Breaking of the Nazis' Codes," The New York Times, 25 October 1974, p. 2.

Randell, B. "The Colossus," A History of Computing in the Twentieth Century, eds., N. Metropolis, J. Howlett, and Gian-Carlo Rota. New York: Academic Press, Inc., 1980, pp. 47-92.

Rejewski, Marian. "Mathematical Solution of the Enigma Cipher," trans. Christopher Kasperek, VI, 1 (January 1982), pp. 1-18.

Rejewski, Marian. "Remarks on Appendix 1 to British Intelligence in the Second World War by F.H. Hinsley," trans. Christopher Kasperek, Cryptologia, VI, 1 (January 1982), pp. 75-83. [Prefatory Note by Richard A. Woytak].

Renauld, P. "La Machine à Chiffrer 'Enigma,'" Bulletin trimestriel de l'Association des Amis de l'Ecole Supérieure de Guerre, No. 78 (2d trimestre 1978), pp. 41-60.

Stengers, Jean. "La Guerre des Messages Codés," L'Histoire, No. 31 (February 1981), pp. 19-31.

Sulzberger, A.O., Jr. "Papers Disclose Allies' Edge in Knowing German Codes," The New York Times, 2 February 1979, p. 13.

Twinn, P.F.G. Letter to the Editor, The Times [London], 21 October 1977, p. 15.

Vincent, E.R. Letter to the Editor, The Times [London], 18 October 1977, p. 17.

Wilkinson, Burke, "British Ear at the German Keyhole." Review of F. W. Winterbotham, The Ultra Secret (Harper and Row). Christian Science Monitor, 3 December 1974, p. 7.

Woytak, Richard A. "A Conversation with Marian Rejewski," trans. Christopher Kasperek, Cryptologia, VI, 1 (January 1982), pp. 50-60.

Woytak, Richard A. "The Origins of the Ultra-Secret Code in Poland, 1937-1938," The Polish Review, XXIII, 3 (1978), pp. 79-85.

UNPUBLISHED MATERIAL

Langer, Gwido. "Wyniki prace: dane dotyczace depesz szyfrowych "Enigma" 6.VII.1939 - 21.VI.1940" ("Summary Data Concerning Deciphered "Enigma" Messages 6 July 1939 - 21 June 1940").

Mayer, Stefan. "The Breaking up of the German ciphering machine "ENIGMA" by the cryptological section in 2-nd Department of the Polish Armed Forces' General Staff," London: 31 May 1974. [Courtesy of Dr. Richard A. Woytak and the Pilsudski Institute, New York].

Mayer, Stefan. "Supplement to the paper of 21.5.1974: "The breaking up of the German ciphering machine Enigma," London: 4 December 1974. [Courtesy of Dr. Richard A. Woytak and the Pilsudski Institute, New York].

INITIAL DISTRIBUTION LIST

	No. Copies
1. Defense Technical Information Center Cameron Station Alexandria, Virginia 22314	2
2. Library, Code 0142 Naval Postgraduate School Monterey, California 93943	2
3. Department Chairman, Code 56 Department of National Security Affairs Naval Postgraduate School Monterey, California 93943	1
4. Professor Stephen Jurika, Code 56 Department of National Security Affairs Naval Postgraduate School Monterey, California 93943	1
5. Professor Boyd Huff, Code 56 Department of National Security Affairs Naval Postgraduate School Monterey, California 93943	1
6. Center for Naval Analyses 2000 North Beauregard Street P.O. Box 11280 Alexandria, Virginia 22311	1
7. Defense Intelligence Agency ATTN: DB-7 (Miss Gouazé) Washington, D.C. 20301	2
8. National Security Agency ATTN: T542 Fort George G. Meade, Maryland 20755	1
9. Defense Intelligence School Washington, D.C. 20301	1
10. Central Intelligence Agency Office of Current Intelligence Room 7G15 Langley, Virginia 20505	1

931-809

206336

Thesis

G588 Gouaze

c.1 Needles and haystacks:
the search for Ultra in
the 1930's.

JUN 11 85

S 12532

206336

Thesis

G588 Gouaze

c.1 Needles and haystacks:
the search for ultra in
the 1930's.



thesG588

Needles and haystacks .



3 2768 001 03529 8

DUDLEY KNOX LIBRARY